REMARKS/ARGUMENTS

This paper is responsive to the Office Action mailed April 8, 2009.

Applicant respectfully traverses the § 103 rejection because the office action has not established a *prima facie* case of obviousness.

Although evidence of a motivation to combine need not be found in the prior art reference themselves, if it is found in the knowledge of one of ordinary skill in the art or, in some cases, from the nature of the problem to be solved, the Office Action must do more than simply discuss the ways that the multiple prior art references can be combined to read on the claimed invention. Rather, the Office Action must point out "specific information in [the two references] that suggest the combination."[1] "'The Board [must] explain what specific understanding or technological principle within the knowledge of one of ordinary skill in the art would have suggested the combination.'"[2]

In *KSR Int'l Co. v. Teleflex Inc. et.al.*[3], the Court re-affirmed that:

Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.[4]

Claims 1 and 7 have been amended in order to introduce that the first auxiliary server comprises confidential data associated to at least one owner of at least one domain name and the second auxiliary server comprises public data associated to at least one domain name.

This new limitation is fully supported by the description, page 6 of the English translation, where it is described that the first server comprises confidential data CONFD and second server comprises public data PUBD.

---

[1] *See Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356,1366, 80 USPQ2d 1641, ___ (Fed. Cir. 2006) (citing *In re Dembiczak*, 175 F.3d 994, 999-1000 (Fed. Cir. 1999)
[2] *Id.* at 1367 (citing *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998))
[3] *Ksr Int'l v. Teleflex, Inc.*, 127 S.Ct. 1727. 82 USPQ 2d 1385 (2007)
[4] Id.

The office action has failed to account for all of the claimed limitations. The combination/modification of the prior art is improper or would not have a reasonable likelihood of success. The prior art has been misinterpreted or mischaracterized. There are no explicit reason(s) why the claimed invention would have been obvious at the time of the invention to one having ordinary skill in the art.[5]

The cited prior art does not teach or suggest all the claim limitations of claims 1 and 7.

The invention relates to a system which ensures a service providing protocol addresses, for example through a DNS, which allows keeping some of the data stored in a database confidential. Data which are kept confidential are data that are associated to a user identifier or a domain name address, such as names, phone numbers and email addresses of owners of the domain name.

Indeed, a DNS server does not filter the information it returns in response to a request identifying a given domain name, so that all data associated with a domain name are returned during a request, which could be for example a "whois" request.

The invention allows exercising a control over the conditions of making public data contained in the database, spreading (partitioning) the data originally contained in the reference server in two groups of data (PUBD, CONFD).

According to this first Office Action, Examiner considers that claims 1 to 7 have to be obviously rejected because of failing to comply with 35USC103(a) considering Shelest et al (US 7,299,491) in view of CERT Coordination Center ("Securing an Internet Name Server") and in further view of Massey et al ("Deploying DNS Security").

Amended claims 1 and 7 clearly claim that the invention uses an architecture (two servers containing various data) which is not disclosed by Shelest in view of CERT Coordination Center.

---

[5] MPEP Sec. 2141, 2142, 2143, 2143.03

The Applicant considers that the document "Massey and Al" which has been used by the Examiner has not a certain publication date. Indeed, the document is supposed to be dated May, 2003 while the real date of publication of the document cannot be proved. It is well known that the real date of publication of documents over the internet can rarely be proved and in the present case, the real date of the document cannot be established.

Furthermore, the disclosure of Massey could not lead to the Invention. Indeed, Massey discloses some security problems in DNS architectures (slides 4 to 7) and some techniques used to overcome these problems. One of these techniques relates to an authentication of a response obtained from a DNS server (after a transmission of a request by a client).

Massey simply explains existing solutions which are used in a secured version of DNS, called "DNSSec". For example, Massey explains the integrity control which is realized on responses (slides 8 and 9): the integrity control is using a signature of the response sent by the server and a verification of the signature by the client which sends the request.

In the invention, as claimed, the security is ensured by an authentication of the client, and a check of an authorization access level associated with the client. The security techniques of the invention never check the responses sent by the servers.

Furthermore, in Massey, there is no mention of a check of an authorization of a client for obtaining public or private data : the goal of Massey is to propose a technique for always giving a response to the client and ensuring that this response is an authenticated one.

Thus, Shelest, when combined with Massey, would lead to a system where the client would be identified before it is requested and the response of the server would be signed for ensuring its authenticity. This is not the object of the invention as claimed in claims 1 and 7, and is not a prima facie case of obviousness.

The Examiner states that CERT provides solutions for securing DNS server, such as "Use Separate Server". It is true that CERT explains that it can be useful to use separate name servers. For CERT, the separate name servers are playing various *roles*, *e.g. various functions as explained page 4.*

On one hand, the first name server is an "Advertising Name Server", e.g. for CERT: *"commonly be used as an external name server that is authoritative for your DNS zones. It would "advertise" this DNS information to the Internet. Since it should not be queried for zones for which it is not authoritative, it should be configured as a non-recursive server. Thus, the server would only provide resolution for the zones for which it has authoritative information"*.

CERT does not explain that the Advertising Name Server comprises some data which are extracted from a reference server. It just explains the function of the Advertising Name Server and the way to realize this function: configuring it as a non-recursive-server, e.g. not allowing it to transfer the request to another Name Server.

On the other hand, the second server is a *"Resolving Name Server which would commonly be used to provide name resolution services to internal clients. It may or may not be configured as authoritative for internal zones. Since it must find DNS information requested by internal hosts (regardless of whether it is authoritative for that information or not), it should be configured as a recursive server. However, it should only answer queries from trusted sources (internal hosts), not from the Internet"*.

Again, CERT does not explain that the Resolving Name Server comprises some data which are extracted from a reference server. It just explains the function of the Resolving Name Server and the way to realize this function: configuring it as a recursive server, e.g. allowing it to transfer the request to another Name Server for obtaining the requested information.

CERT never discloses, explains or suggests that *"the information that is normally on one server is distributed according to the criteria disclosed."*

The Applicant respectfully disagrees with the arguments of the Examiner because CERT does not explain that the data are spread out from a reference server. CERT just explains how to manage queries (recursive, non-recursive) and never explains that the first server comprises a first database with a first set of data (public) and the second server comprises a second database with a second set of data (private) and that these data are issued for a reference server. Indeed, CERT does not even mention the "Reference Server."

When searching to solve the problem of security of name servers on the Internet, the one of ordinary skill in the art would have considered "Shelest". From "Shelest", *which already solves this problem (see "Shelest" col. 4, lines 55-60)*, the one of ordinary skill in the art:

> would have learned that a client authentication check can be done (fig 4, step 420) on a server (which is not told to be a reference server, because in "Shelest" there is only one server, which is the one which is realizing the authentication process with the client), col. 4, lines 51 to 66, and that, if the client does not have an authentication, the response is an "unknown domain name" response.

From CERT, one of ordinary skill in the art would have learned that, to further increase the security:

a)   some filtering process can be used to filter the traffic (page 5 of CERT);

b)   it is possible to use separate servers where:

> an "Advertising Name Server" is commonly used as an external name server that is authoritative for the one of ordinary skill in the art DNS zones;

> a "Resolving Name Server" is commonly used to provide name resolution services to internal clients.

This would lead the ordinary skilled in the art to a system comprising an Advertising Name Server which would be used to answer the client which has no authentication by not authorizing recursive search from the Advertising Name Server.

The system would also comprise a Resolving Name Server which would check a client authentication, and if the client does not have an authentication, the response is an "unknown domain name" response.

The system which is obtained does not meet all the limitations of claims 1 and 7. Indeed, claims 1 and 7 differ from the previous system at least because in claims 1 and 7 the data included in the first and the second auxiliary servers are data issued from the reference server and these data issued from the reference server are spread over both

auxiliary servers relative to the first and the second authorization access level attributed to the data.

Thus, the system which is obtained by the presently claimed invention is not a prima facie case of obviousness according to the Supreme Court Decision in KSR International Co. vs Teleflex[6].

Thus Claims 1 and 7 are inventive in view of Shelest and CERT.

Even if the Examiner could find some arguments proving a prima facie case of obviousness, despite the previous demonstration, the amendment in claims 1 and 7 to precise the contents of the data which are *(intentionally)* spread out between first and second auxiliary server and are not the result of the copy of data coming from other servers.

Indeed, when a Name Server is configured as "Resolving Name Server", e.g. it is configured to find an IP address of a domain Name it is well known (see Wikipedia: http://en.wikipedia.org/wiki/Domain_Name_System) the "Resolver" can effectively cache some responses obtained for the resolution of some queries.

But, the cached data are issued from former queries received by the Resolver and, as a result, the data are not spread out according to authorization access level attributed to the data, and moreover, the data are not spread out to put the private data of the owner in one server and the public data of the owner in another server.

As a consequence, as "Shelest" does not disclose a system for managing personal data of domains names owners or technical data and "Shelest" in view of CERT does not disclose all the limitations of claims 1 and 7.

---

[6] 550 U.S. – 82 USPQ2d 1385 (2007)

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 02-3732.

Respectfully submitted,

Dated: _8 July 09_

By _[signature]_
Gerald E. Helget (Reg. No. 30,948)
Nelson R. Capes (Reg. No. 37,106)
BRIGGS AND MORGAN, P.A.
2200 IDS Center, 80 South Eighth Street
Minneapolis, MN 55402
Telephone: 612-977-8480
Facsimile: 612-977-8650